

OSC



오픈소스 거버넌스 자동화와
소프트웨어 공급망 관리

OSC Korea | Sonatype 한국 총판

750k

매주 릴리즈 되는 신규 오픈소스

100k

매주 식별되는 새로운 보안위협

2,689

관리대상 오픈소스 라이선스 종류

27 Days

NVD에서 CVE 등록에 소요되는 시간



01. 소프트웨어공급망 관리의 도전과제 및 공격 기법

02. 오픈소스 거버넌스 자동화 고려사항

03. 오픈소스 거버넌스 자동화 구현 방안

04. SBOM 통합관리를 위한 SBOM Manager

Software Supply Chain Challenges & Attacks

- ✔ 소프트웨어 공급망 관리의 도전과제 및 공격 기법
- ✔ 오픈소스 거버넌스 자동화 고려사항
- ✔ 오픈소스 거버넌스 자동화 구현 방안
- ✔ SBOM 통합관리를 위한 SBOM Manager

오픈소스 거버넌스 영역의 전개

2000's : 라이선스



각종 라이선스 분쟁

2010's : 취약점



취약점을 이용한 대형 보안침해 사고

2020's : 멀웨어



공급망을 통한 악성코드/멀웨어 공격패턴 급증



라이선스 관리

관리대상 라이선스 종류 : 2,689 종 (24년 8월)

❖ 라이선스 관리의 복잡성

- 오픈소스 도입 초기에는 관리할 의존성이 많지 않았고, 라이선스 종류도 많지 않았음 (MIT, BSD, GPL/AGPL, Mozilla)
- 프로젝트당 평균 +150여개의 오픈소스를 사용하고 라이선스의 종류도 지속적으로 많아지고 있음
- 라이선스별 요구사항을 파악하고 고지의무 등을 준수하기 위해 자동화된 도구의 사용이 필요함

Root Organization
Policy Management

- ▶ Application Categories
- ▶ Policies
- Legacy Violations
- Continuous Monitoring
- Proprietary Components
- ▶ Component Labels
- ▼ License Threat Groups
 - + New License Threat Group
 - Banned
 - Copyleft
 - Commercial
 - Non Standard
 - Sonatype Special Licenses
 - Weak Copyleft
 - Liberal
 - Sonatype Informational
- Source Control
- ▶ Access

Edit License Threat Group

Group Name * ● 10 - Critical

Available Licenses

Filter

- + (0BSD) BSD Zero Clause Lice...
- + (10tec-Company-License-Agr...
- + (123-OSO-MIT-PL-2.0) 123 Op...
- + (2KSYS-EULA) 2KSYS End Use...
- + (3D-Slicer) 3D-Slicer-Style Lic...
- + (3D-Slicer-1.0) 3D Slicer Licen...
- + (42-Unlicense) 42 Unlicense
- + (60East-API-LA) 60East API Li...
- + (AAL) Attribution Assurance ...
- + (AB-CPSign-Commercial-EUL...

2411 Licenses available

Included Licenses

Filter

- + (AbtAudio-AB-License) AbtAu...
- + (Accusoft-SLA) Accusoft Tool...
- + (ACSL) ACSL-Style License No...
- + (ACSL-1.4) Anti-Capitalist Soft...
- + (AdGem-User-TOS-RD020220...
- + (AGPL) AGPL-Style License N...
- + (AGPL-1.0) Affero General Pu...
- + (AGPL-1.0-or-later) Affero Ge...
- + (AGPL-2.0) Affero General Pu...
- + (AGPL-3.0) GNU Affero Gener...

278 Licenses transferred

Local to Root Organization

● 10	Banned	>
● 9	Copyleft	>
● 7	Commercial	>
● 6	Non Standard	>
● 5	Sonatype Special Licenses	>
● 2	Weak Copyleft	>
● 0	Sonatype Informational	>
● 0	Liberal	>

Banned	Copyleft	Commercial	Non Standard	Weak Copyleft	Liberal
278	61	927	131	202	78
					

소프트웨어 공급망을 통한 보안 위협

Flaws



Foes



01. Vulnerability (취약점)

악용(Exploited)될 수 있는 결함으로 인해 취약한 컴포넌트

CVE 로 관리

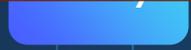
침해 행위가 일어나는 경우 피해

02. Malware (악성코드)

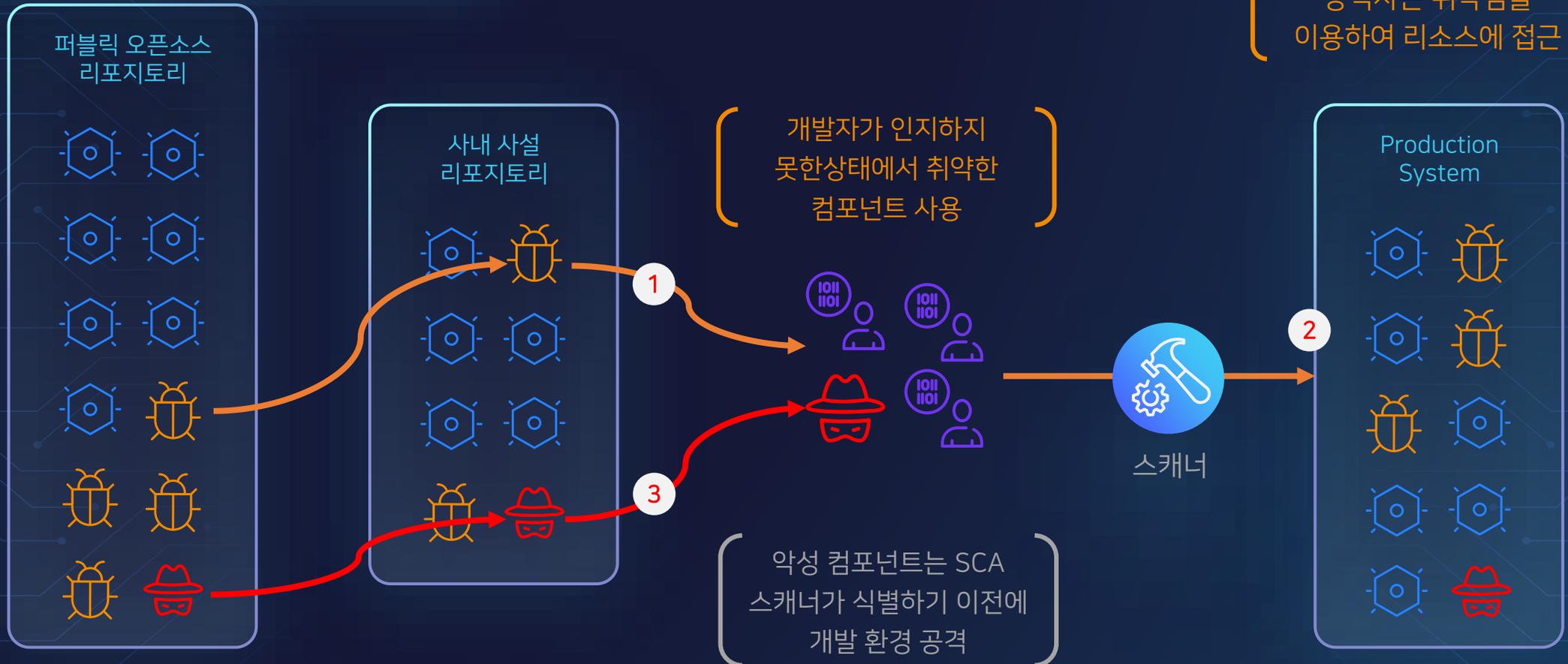
유해한 코드를 주입하기 위해 의도적으로 만들어진 악성 컴포넌트

CVE로 관리되지 않음

내부로 유입되면 즉각적인 피해



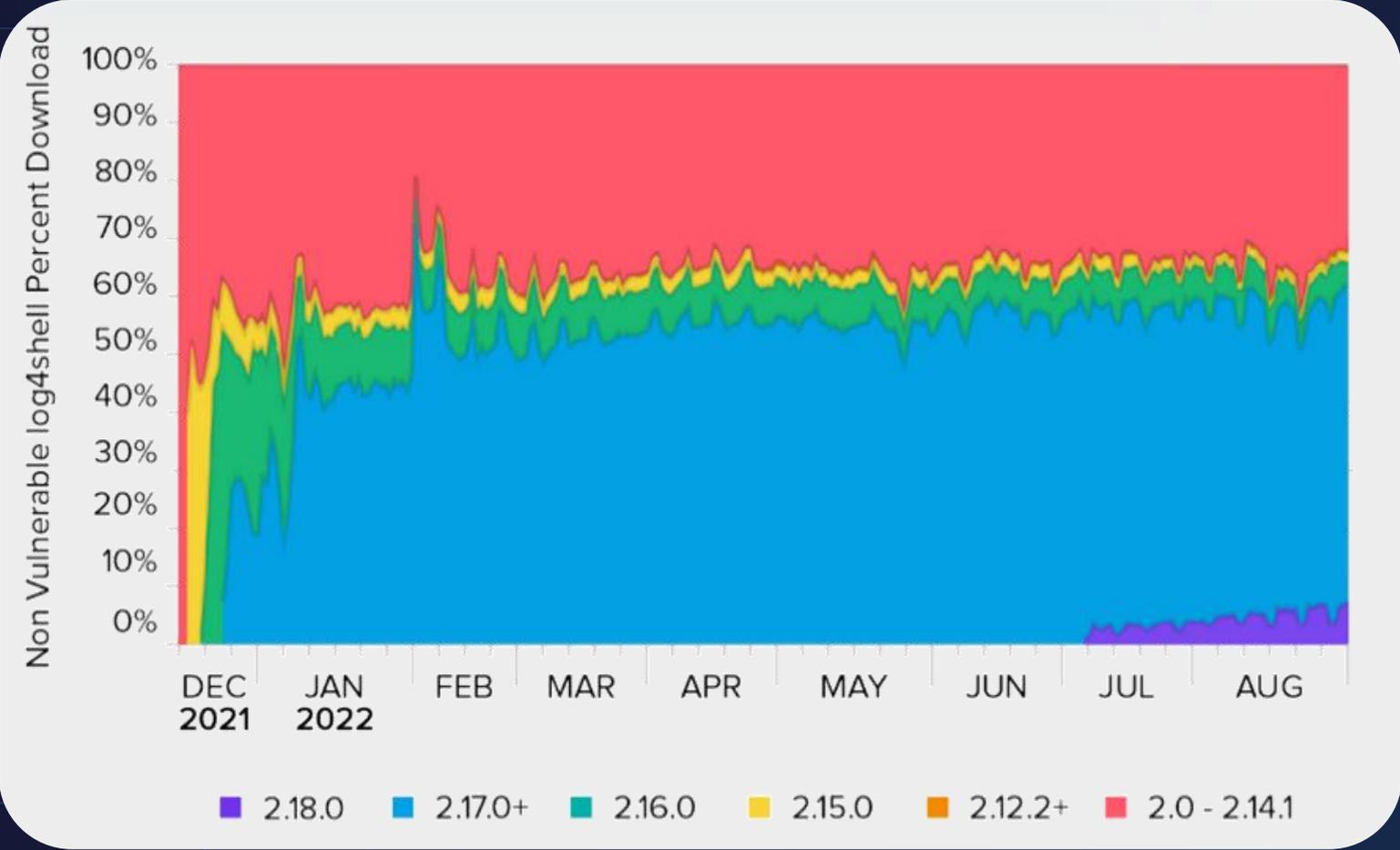
개발환경의 위협요소



-  취약 컴포넌트
-  악성 컴포넌트

내부 개발환경

취약 컴포넌트 다운로드 현황



2021년 Log4j 취약점이 공개된 후 개선된 버전이 다수 릴리즈 되었지만 여전히 취약한 버전의 다운로드 비중이 30%를 차지함

Source: Log4Shell Vulnerable Downloads - Sonatype (Maven Central)

타이포스쿼팅

- 주요 패키지명의 타이핑오류를 활용하는 기법
- 정상 패키지와 비슷하게 보이는 악성 패키지를 만든 후, NPM Repository 등에 업로드
- 개발자들이 의존성을 정의할 때 이름을 잘못 입력하는 경우, 의도된 악성 패키지가 다운로드 되어 공격에 이용되는 방식
- 배치 스크립트는 윈도우의 레지스트리를 변경하거나, 트로이목마 또는 랜섬웨어를 통해 대상 호스트를 감염시킴



I NEEVR
MAKE TYPOS

1 타이포스쿼팅 예시

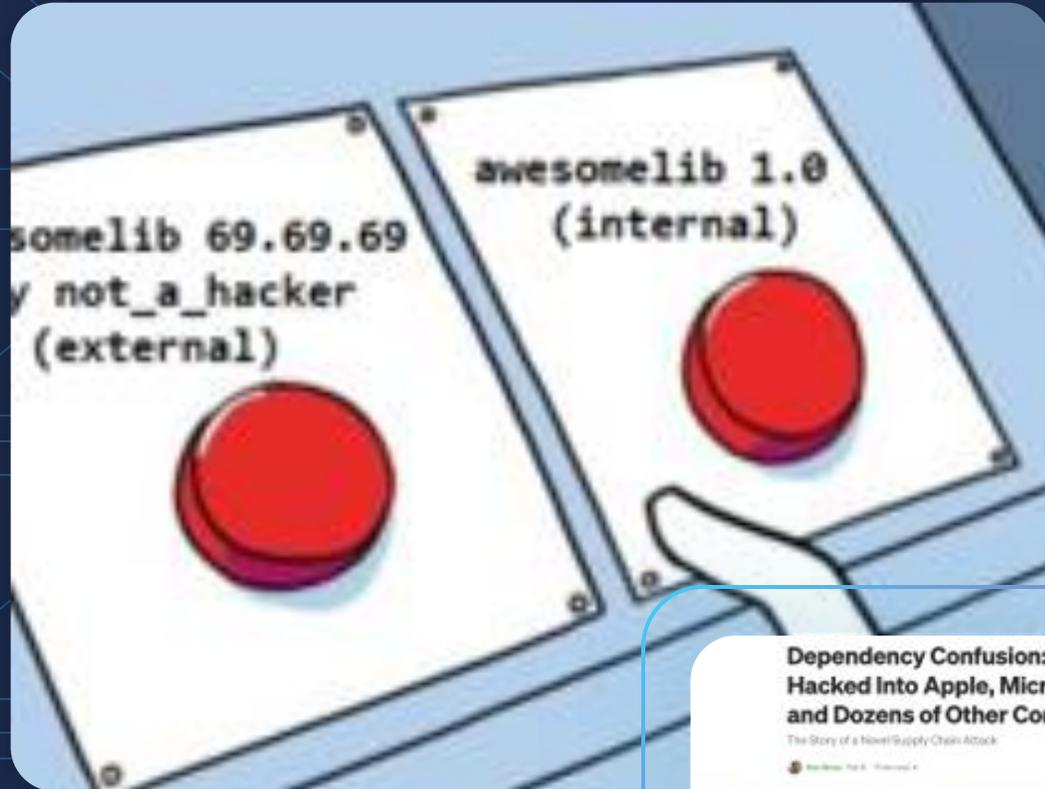
1. cross-env -> crossenv
2. express -> exprss
3. electron -> electorn

2 공격 형태

1. Data exfiltration (데이터 탈취)
2. Code Injection (코드 삽입)
3. Crypto Stealer / Miner (암호탈취 / 마이닝)
4. Denial of Service (서비스 거부공격)
5. Obfuscated Code (난독화 코드)
6. Backdoor Install (백도어 설치)
7. File System Corruption (파일시스템 손상)

3 최근 사례 (2024년 8월)

1. 정식 프로젝트 (블록체인 지원 Python APIs)
 - Github : solana-py v0.34.3
 - PyPI : solana
2. 악성 코드 배포
 - PyPI : solana-py v0.34.5
 - 전자지갑 암호 키 탈취



Dependency Confusion (의존성 혼동)

❖ Alex Birsan (2021년)

- 공개 저장소의 보안강화 이후 다른 형태의 Supply Chain 공격 방식 등장
- 내부 어플리케이션에서 사용하는 패키지명을 찾아낸 후 내부의 낮은 버전보다 외부 최신 Dependency를 우선하는 패키지 매니저의 특성을 활용한 기법
- 피해기업 : Apple, Microsoft, Netflix, PayPal, Shopify, Tesla and Uber 회사 등

Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies
The Story of a Novel Supply Chain Attack



❖ PyTorch (2022년)

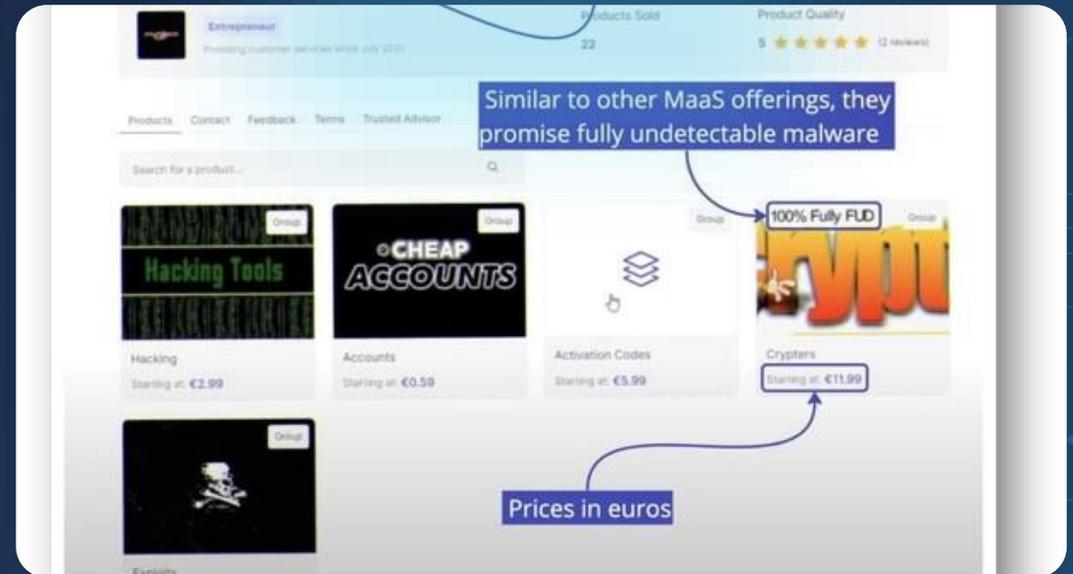
- PyTorch-nightly 빌드가 사실 저장소에서 패키지 (torchtriton)를 다운받는 허점을 이용해 공식 저장소에 동명의 악성 패키지를 높은 버전으로 업로드 함
- Python 공식 저장소(pypi.org)가 사실 저장소보다 우선하여 악성 패키지가 일반 사용자에게 배포됨

Malicious Code Injection (악성코드 주입)

Malicious Code Injection

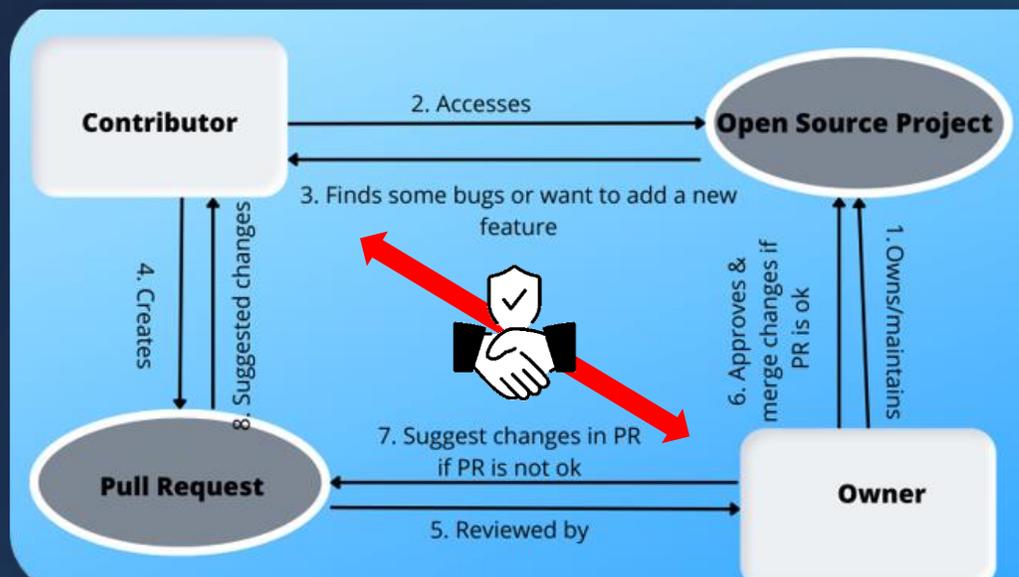


Malware as a Service



정상 프로젝트를 통한 잠입

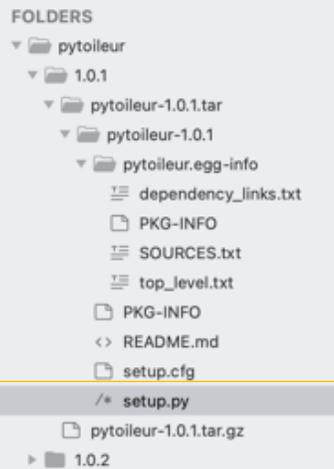
“활동이 적은 프로젝트의 관리 허점을 찾거나 프로젝트 Owner와 신뢰관계를 구축하여 Commit 권한 획득”



PyPI crypto-stealer targets Windows users, revives malware campaign

May 29, 2024 By [Ax Sharma](#)

7 minute read time

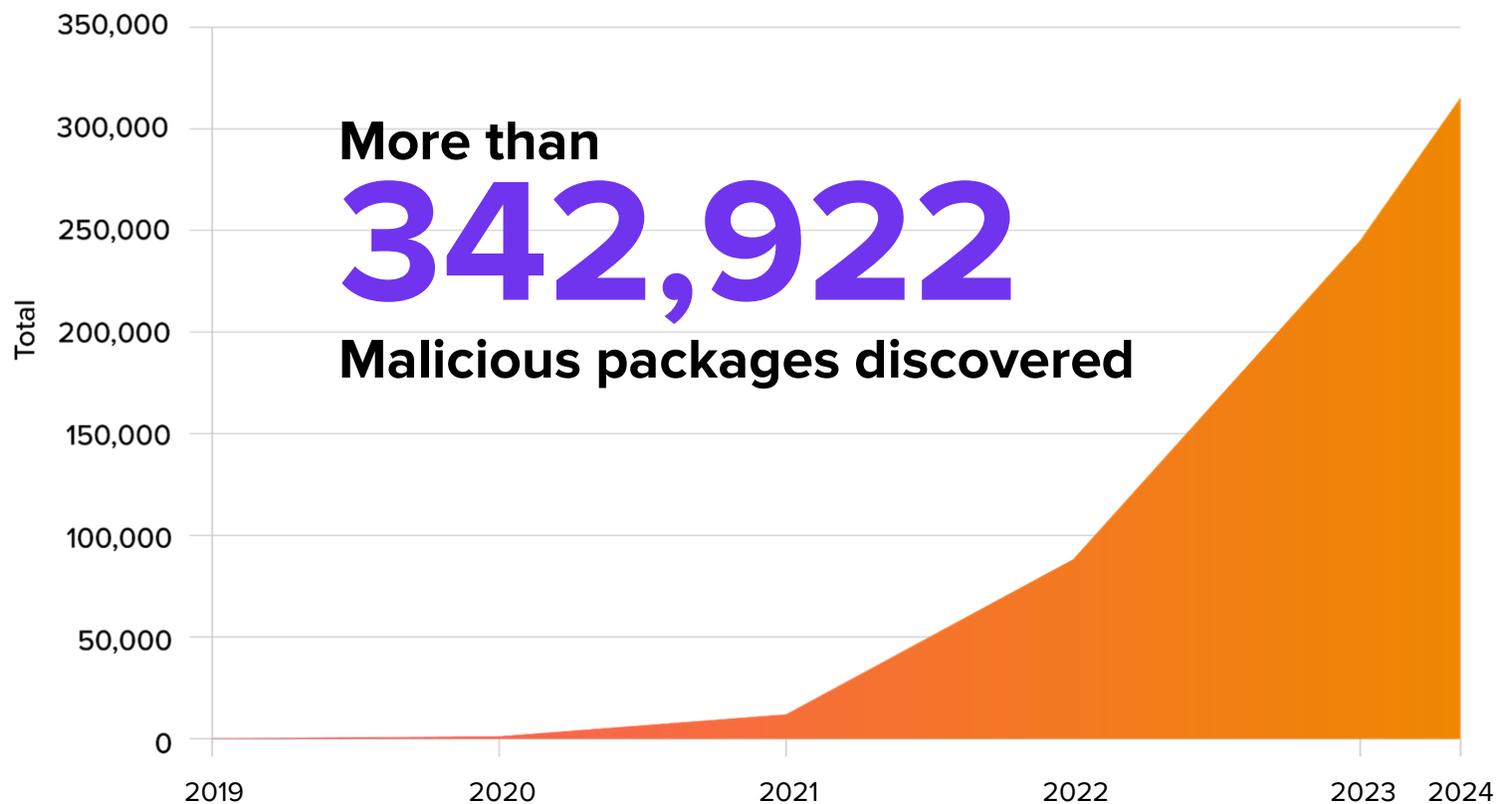


```
setup.py
1 from setuptools import setup, find_packages
2 from setuptools.command.install import install
3 from pathlib import Path
4 import os
5
6
7 VERSION = '1.0.1'
8 DESCRIPTION = 'Cool package.'
9 this_directory = Path(__file__).parent
10 long_description = (this_directory / "README.md").read_text()
11
12
13 class InstallCommand(install):
14
15     def run(self):
16         try:
17             print("")
18         except:
19             pass
20         install.run(self)
21
22
23 setup(
24     name="pytoileur",
25     version=VERSION,
26     author="HW",
27     author_email="",
28     description=DESCRIPTION,
29     long_description_content_type="text/markdown",
30     long_description=long_description,
31     packages=find_packages(),
32     install_requires=[],
33     keywords=[],
34     classifiers=[
35         "Development Status :: 1 - Planning",
36         "Intended Audience :: Developers",
37         "Programming Language :: Python :: 3",
38         "Operating System :: Unix",
39         "Operating System :: MacOS :: MacOS X",
40         "Operating System :: Microsoft :: Windows",
41     ],
42     cmdclass={
43         'install': InstallCommand
44     }
45 )
```



base64-encoded payload
실행 명령어

악성 소프트웨어를 통한 공급망 공격 현황



2023년에는 이전해까지 발견된 모든 악성패키지의 **2배**에 달하는 악성패키지가 탐지됨

악성 소프트웨어 식별 및 대응 속도

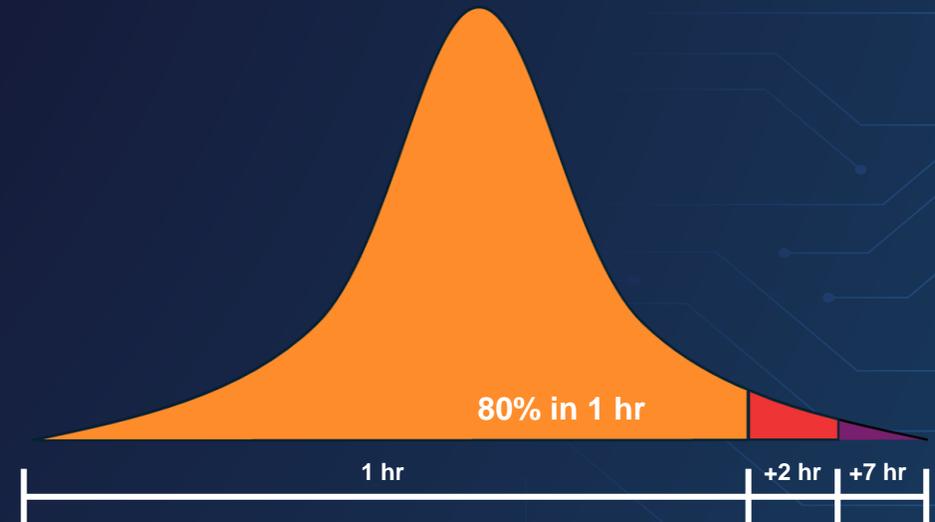
342,922
malicious versions

Sonatype
Discovered **289,933**



- Phishing **96,465**
- Data Exfiltration **73,008**
- Security Holding **64,779**
- Other **31,652**
- PII Exfiltration **19,772**
- Backdoor **13,065**
- Research Project **8,421**
- PUA **7,669**
- Crypto Stealer/Miner **4,837**
- Dropper **4,734**
- File System Corruption **2,212**
- Protestware **1,067**
- Code Injection **911**
- Denial of Service **848**
- Credential Exfiltration **600**
- Obfuscated Code **204**
- Ransomware **37**
- Hijacker **19**
- URL Redirector **8**

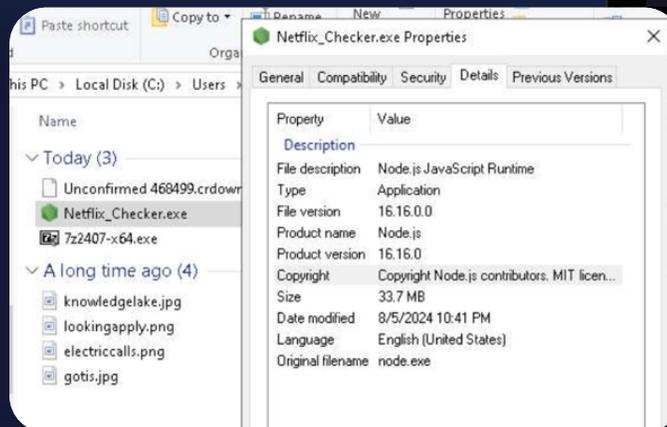
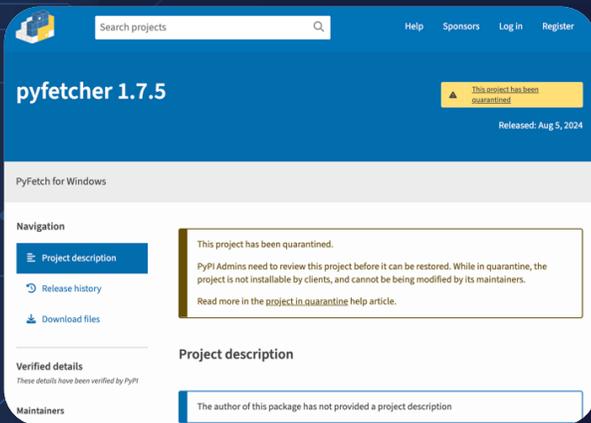
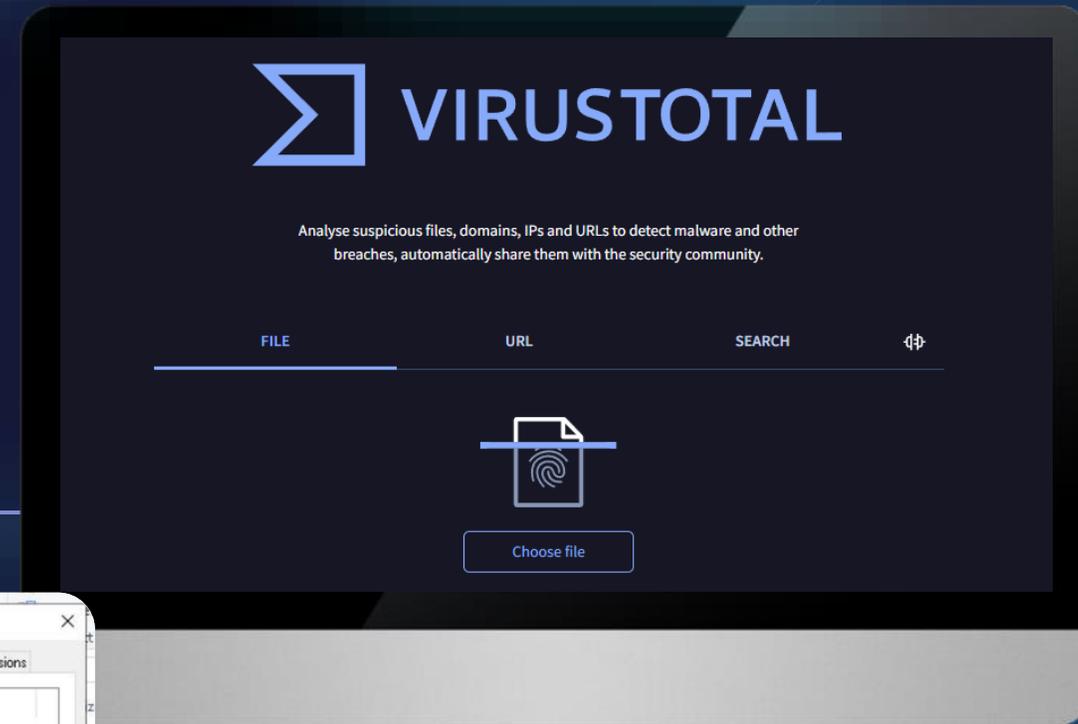
식별된 악성소프트웨어 중 **80%**는
1시간 내에 Sonatype Database에
추가



소프트웨어 공급망 vs. Anti-Virus

Anti-Virus 검색 결과 > Undetected

- Sonatype 보안팀에서 탐지한 악성 PyPI 패키지 (netfetcher, pyfetcher)
- 동명의 윈도우 유틸리티를 가장하여 특정 URL로부터 악성 실행 화일을 다운로드 후 이름 변경 (netflix_checker.exe)
- 공식 NodeJS 로고와 메타데이터 포함하여 공식 패키지로 가장
- 2024년 8월 22일 현재 C2서버 Active 상태
- Anti-Virus 도구에서 탐지 되지 않음



출처 : <https://www.sonatype.com/blog/pyfetcher-netfetch-drop-netflix-checker-on-windows>

Governance Automation Consideration

- ✔ 소프트웨어 공급망 관리의 도전과제 및 공격 기법
- ✔ 오픈소스 거버넌스 자동화 고려사항
- ✔ 오픈소스 거버넌스 자동화 구현 방안
- ✔ SBOM 통합관리를 위한 SBOM Manager

오픈소스 거버넌스 자동화 요건

오픈소스 거버넌스의 자동화는 고품질의 데이터를 기반으로 정확하게 오픈소스 컴포넌트를 식별하여 오탐이 없는 환경을 구축하고, 단계별 정책을 적용하여 전 방위적인 리스크 관리체계 확보를 목표로 함



고품질 데이터베이스 확보 방식

Automated Vulnerability Detection



Public Sources : Security Feeds & Others

- CVE Feeds
- 보안 공지사이트 (Security Advisories)
- 프로젝트 보안 공지
- FSISAC & Customer Report
- Email, Blog, OWASP, OSSIndex

Github 모든 오픈소스 Commit / Event 모니터링

- CVE, SQL Injection, XXE, RCE, XSS

60여개 시그널을 통한 AI/ML 기반 Behavior 모니터링

- Public Repository (NPM, PyPI, Maven등) 24X7 감시

Human Curation



Sonatype 보안 리서치팀 Curation (+65명)

- 소스코드 분석 (Class, Method)
- 보안이슈(Defect)의 근본 출처 확인
- 불일치(Discrepancy), 모호함(Vagueness), 부정확성 (Inaccuracy) 제거

Deep Dive 정보 추가

- Sonatype (정보 소스) 고유정보 추가
- Remediation 추가

추가 정보 수집

- Github 및 프로젝트 다운로드 사이트 분석
- 인기도, Release History, Declared License

Secondary Expansion



추가 분석 및 취약점간 상호 연계

- 신규 취약점에 대해 기존 다른 컴포넌트에 미치는 영향 추가 분석
- 해당 취약점이 복수의 라이브러리에 영향을 미치고 있는지 확인
- Secondary Expansion 분석을 통해 현재까지 3,800만개의 취약점 정보 추가

오탐 방지 효과

- False Negative : 0.1%
- False Positive : 0.6%

Sonatype Data Story - 주요 지표



Breadth

270M **8M/Day**
오픈소스 카탈로그 Github/보안공지



Depth

55M **14M**
취약점 데이터 Deep Dive (심층분석)



Speed

10 mins **1 Hour**
OSS 카탈로그 악성패키지



Accuracy

32%
Sonatype 에서 수정한
퍼블릭 보안공지



Sonatype Data 품질 평가 사례 #1 (False Positive)

점검대상	레퍼런스 CVEs	Sonatype 점검결과
spring-core-5.3.5.jar	CVE-2023-20863	spring-expression
	CVE-2023-20861	spring-expression
	CVE-2022-22971	spring-messaging
	CVE-2022-22970	spring-beans
	CVE-2022-22968	spring-context
	CVE-2022-22965	spring-beans
	CVE-2022-22950	spring-expression
	CVE-2021-22118	spring-web
	CVE-2021-22096	spring-web
	CVE-2021-22060	spring-webmvc, spring-webflux, spring-websocket

MVN REPOSITORY
 Indexed Artifacts (35.3M)
 Home » org.springframework » spring-core » 5.3.5
Spring Core » 5.3.5
 Basic building block for Spring that in conjunction with Spring Beans provides dependency injection and IoC features.
 License: Apache 2.0
 Categories: Core Utilities
 Tags: spring, framework
 Organization: Spring IO
 HomePage: https://github.com/spring-projects/spring-framework
 Date: Mar 16, 2021
 Files: pom (1 KB) | jar (1.4 MB) View All
 Repositories: Central
 Ranking: #62 in MvnRepository (See Top Artifacts) | #4 in Core Utilities
 Used By: 8,385 artifacts
Vulnerabilities
 Direct vulnerabilities:
 CVE-2023-20863
 CVE-2023-20861
 CVE-2022-22971
 CVE-2022-22970
 CVE-2022-22968
 CVE-2022-22965
 CVE-2021-22096
 CVE-2021-22060

Vulnerability Lookup

Find Results on Specific Vulnerabilities

All vulnerability lookups must use an exact match to surface a result.

Input: CVE-2023-20863

Find

Result: CVE-2023-20863 (Deep Dive)

Issue
[CVE-2023-20863](#)

Severity
 CVE CVSS 3: 6.5
 Sonatype CVSS 3: 7.5

Weakness
[CVE CWE: 917](#)

Source
 National Vulnerability Database

Categories
 Data
 Operational

Description from CVE
 In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

Explanation
 The `spring-expression` package is vulnerable to Denial of Service (DoS) attacks. The `doParseExpression()` method in the `InternalSpelExpressionParser` class fails to limit the length of SpEL expressions before attempting to parse them. A remote attacker who can supply crafted SpEL expressions can leverage this behavior to cause the application to exhaust its available resources and ultimately induce a DoS condition.

Detection
 The application is vulnerable by using this component.

Recommendation
 We recommend upgrading to a version of this component that is not vulnerable to this specific issue.

Advisories
 Project: <https://github.com/spring-projects/spring-framework/issues/30325>
 Project: <https://spring.io/security/cve-2023-20863>

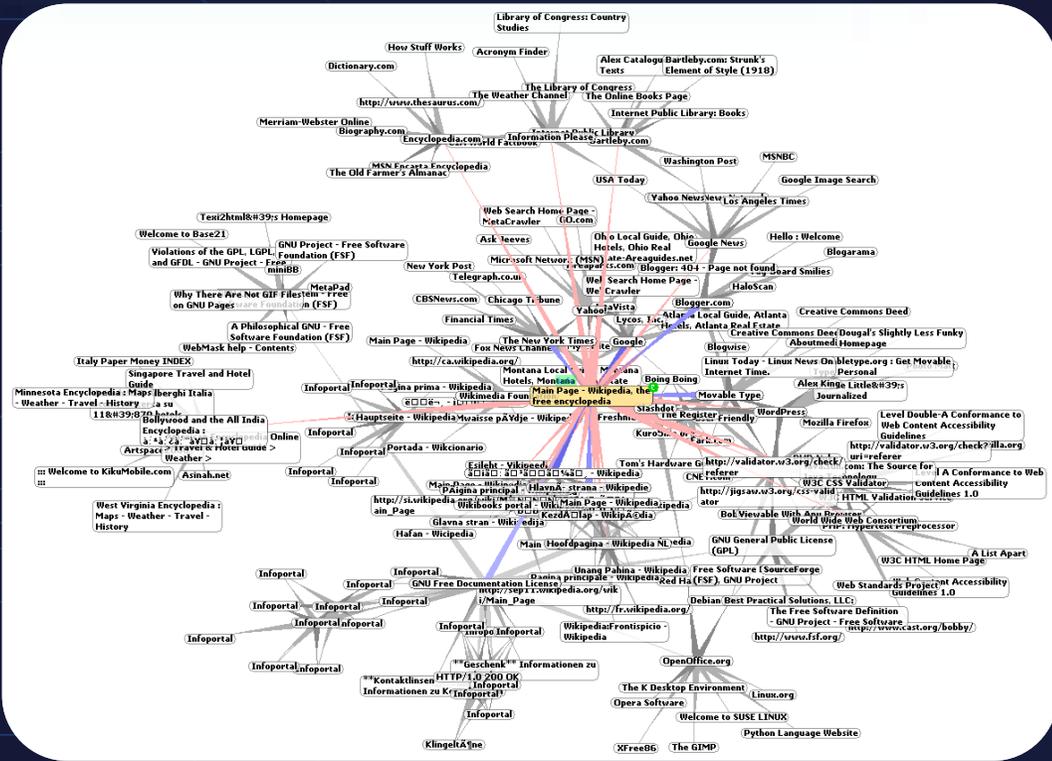
CVSS Details
 CVE CVSS 3: 6.5
 CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

- MVN Repository 포털에는 Spring Core에 대한 CVE들이 기록되어 있으나 실제 해당 CVE들은 Spring Core가 아닌 다른 컴포넌트에 대한 CVE들입니다.
- Public 데이터에 만 의존한 진단을 수행하는 솔루션의 경우에는 오탐 (과탐 : False Positive)을 유발하게 됩니다

Governance Automation Implementation

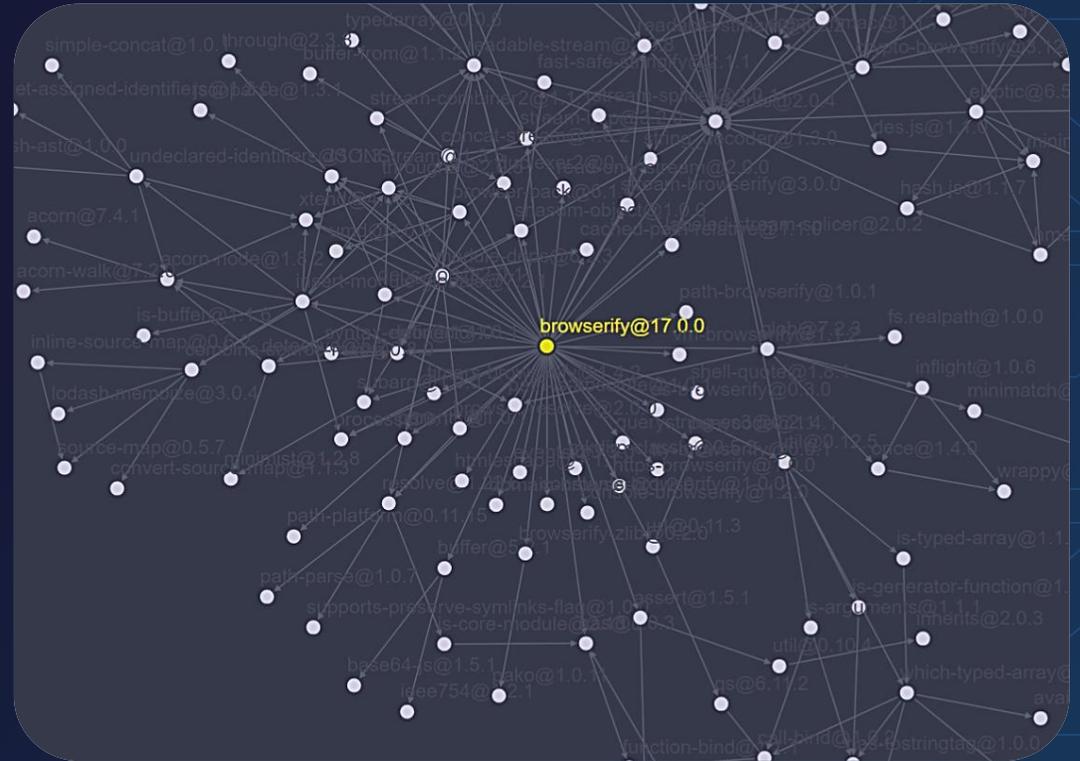
- ✔ 소프트웨어 공급망 관리의 도전과제 및 공격 기법
- ✔ 오픈소스 거버넌스 자동화 고려사항
- ✔ 오픈소스 거버넌스 자동화 구현 방안
- ✔ SBOM 통합관리를 위한 SBOM Manager

오픈소스 거버넌스 특성



Web Hyperlink

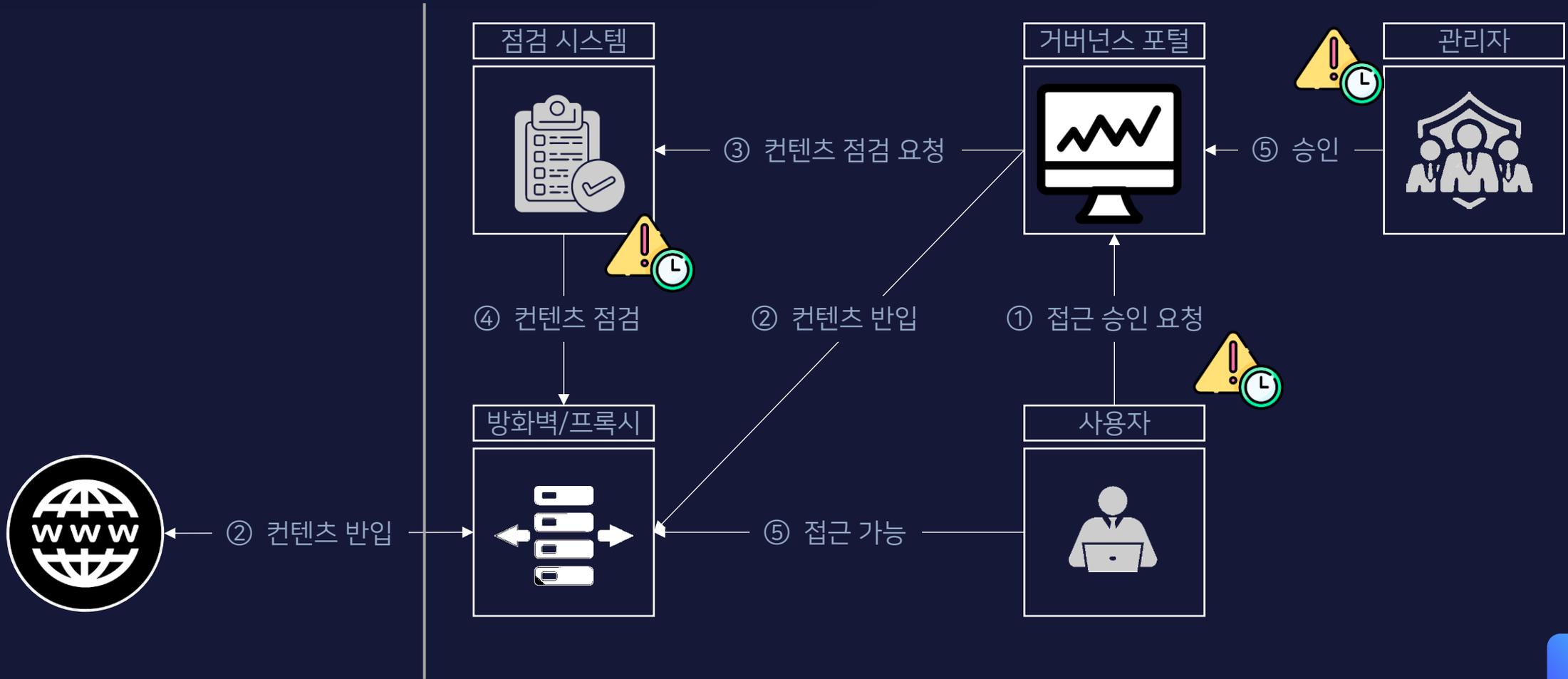
https://en.wikipedia.org/wiki/World_Wide_Web



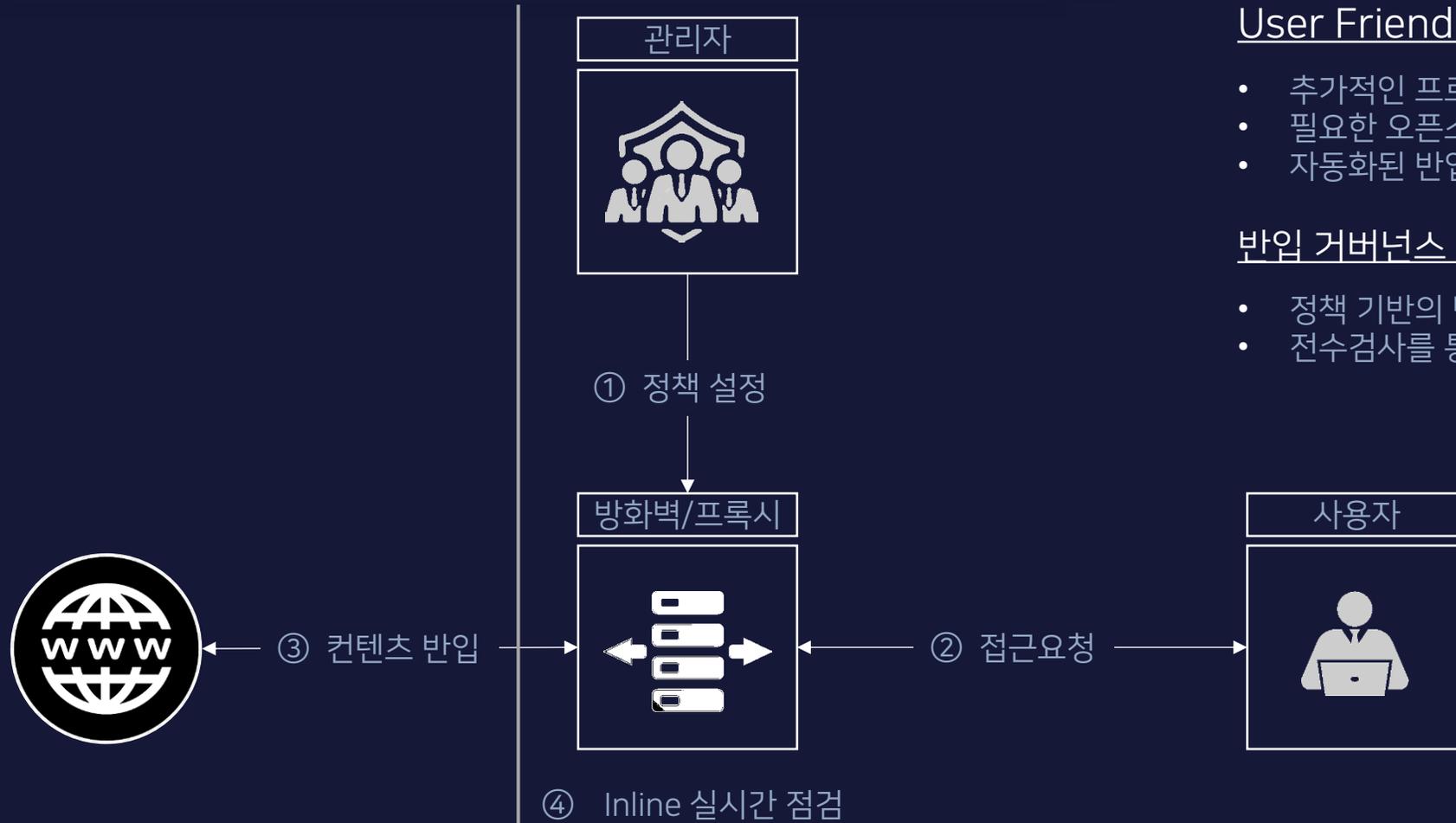
Dependency (의존성)

<https://npm.anvaka.com/#/>

거버넌스 구현 방식 비교 - 포털 방식



거버넌스 구현 방식 비교 - Inline 방식



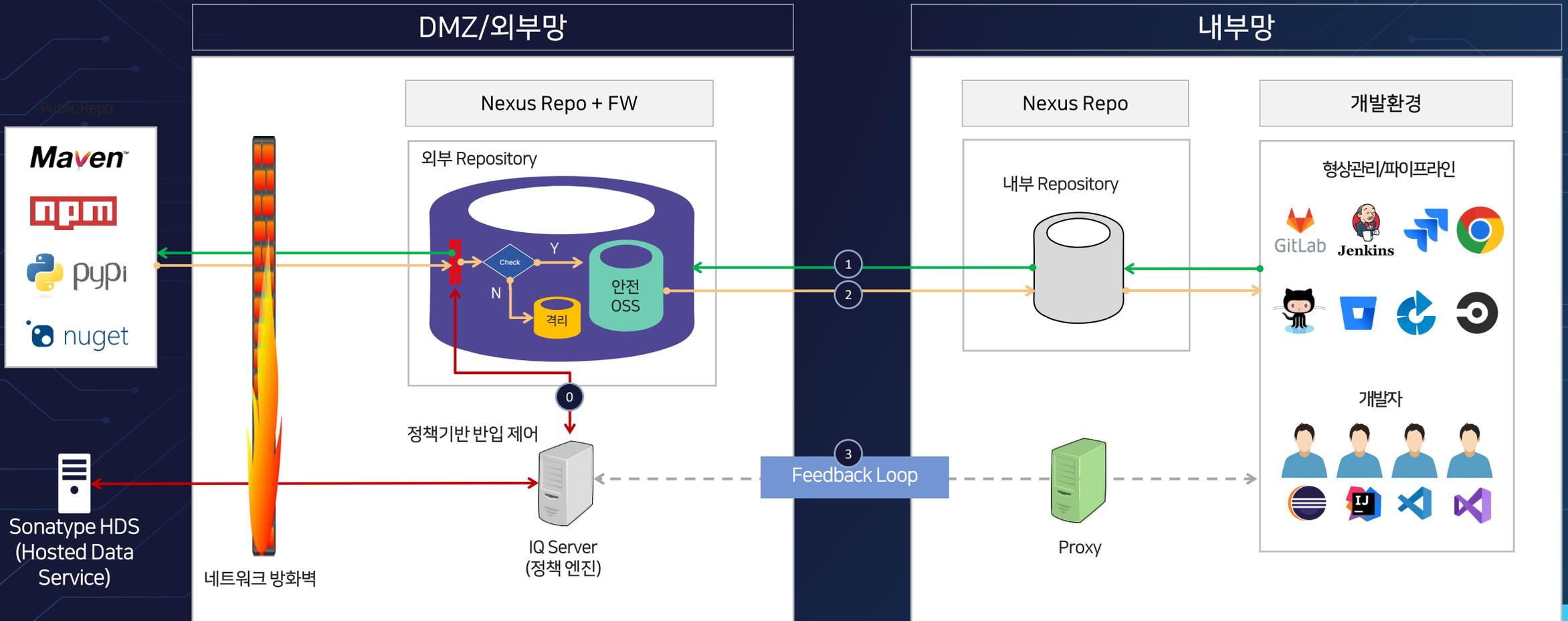
User Friendly

- 추가적인 프로세스 필요 없음
- 필요한 오픈소스를 즉시 활용하여 생산성 향상
- 자동화된 반입 프로세스로 개발시간 단축

반입 거버넌스 자동화

- 정책 기반의 반입 거버넌스
- 전수검사를 통해 오픈소스 리스크 감소

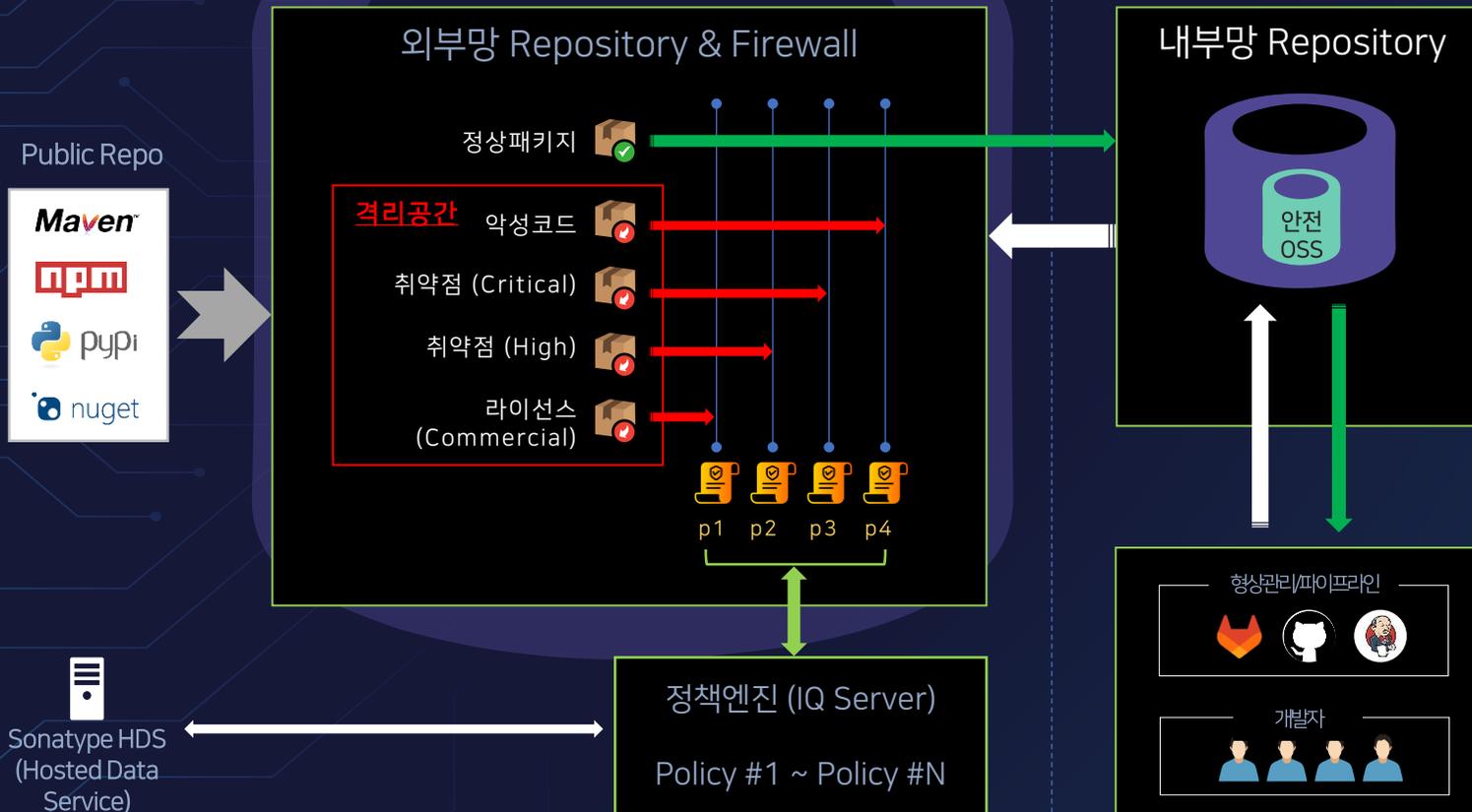
Sonatype Platform 표준 구성 (Repo + FW)



정책설정을 통한 반입통제 자동화

- Nexus상에 FW 기능 탑재로 반입 오픈소스 전수 검사
- 악성코드/멀웨어, 라이선스 및 취약점을 정책 기반으로 통제

- 개발자는 기존 프로세스의 변경 없음
- 자동화된 거버넌스 정책 적용으로 관리비용 절감



Developer Friendly

- 신규 오픈소스를 사용하기 위해 추가적인 프로세스 필요 없음
- 사전 신청 및 승인 과정이 필요 없으므로 개발자 생산성 향상
- 자동화된 반입 프로세스로 개발시간 단축

반입 거버넌스 자동화

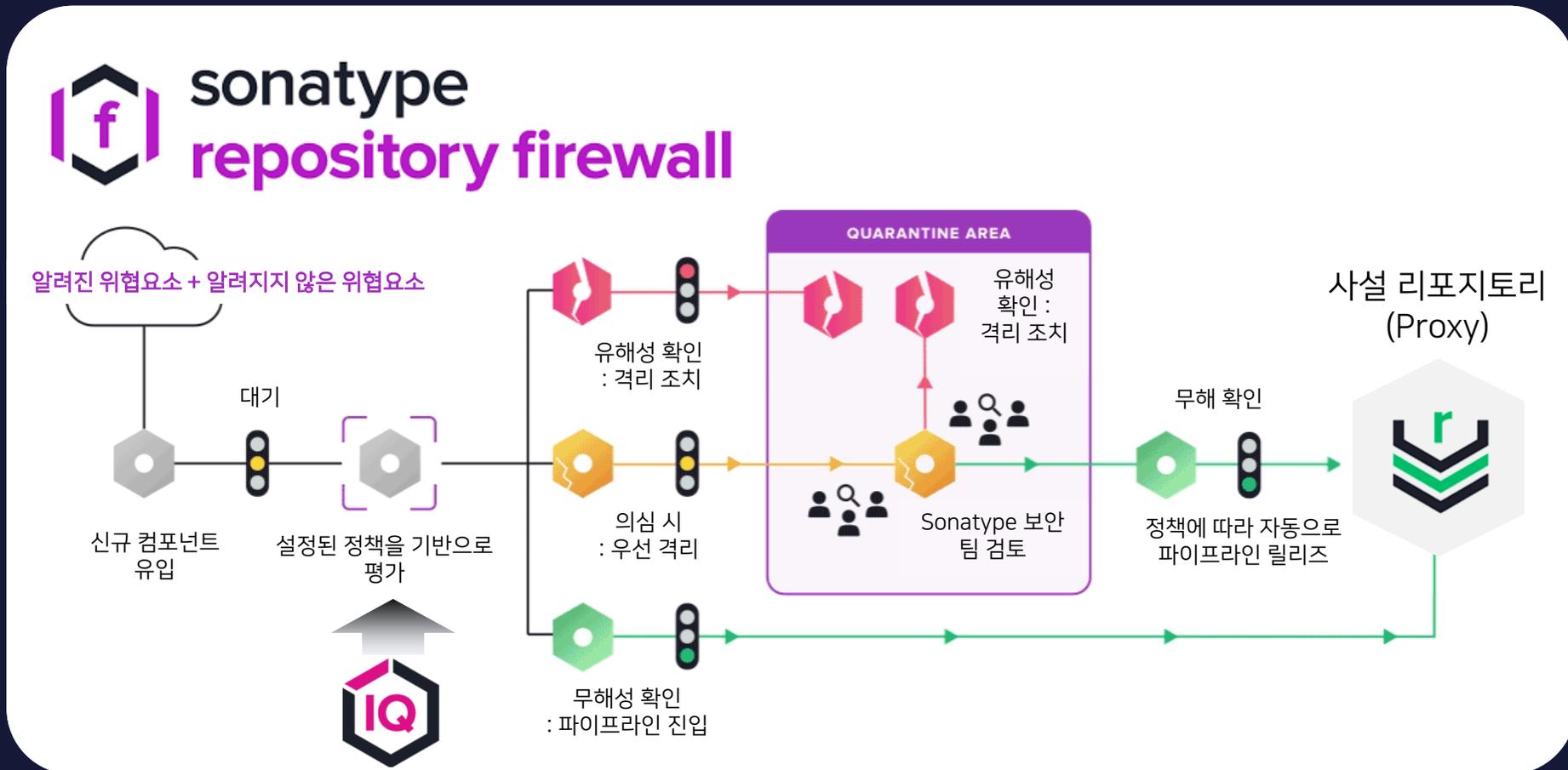
- 전사차원의 일관된 반입 정책 수립
- 사전 정의된 정책을 기반으로 반입 패키지에 대한 전수검사

안전한 오픈소스 사용환경 확보

- 글로벌 최대 데이터베이스를 기반으로 악성코드/멀웨어 원천 차단

Sonatype Repository Firewall

60여개의 시그널을 분석하는 AI/ML 알고리즘을 통해 소프트웨어 공급망을 24X7X365 모니터링 하며 유입되는 오픈소스를 평가하여 유해한 것으로 판단되는 경우 자동으로 다운로드 차단



패키지 차단 시 개발자 조치 : Self Remediation

```
Last login: Fri Feb 18 16:01:53 on ttys003
nnandivelugu@Navyasanthis-MacBook-Pro ~ % npm install 1gallery@0.0.8
npm WARN enoent ENOENT: no such file or directory, open '/Users/nnandivelugu/package.json'
npm WARN nnandivelugu No description
npm WARN nnandivelugu No repository field.
npm WARN nnandivelugu No README data
npm WARN
빌드 에러 개발자 화면에서 확인 -> 조치 URL 제공
npm ERR! code E403
npm ERR! 403 403 ----->>> REQUESTED ITEM IS QUARANTINED -----
----->>> FOR DETAILS SEE ----->>> http://localhost:8072/ui/links/repositories/quarantinedComponent/MWU1YjRhYTA3ODNmNGE0WE40WNmYzA0YjlkNzEwMzQ0 <<<-----
- GET http://localhost:8081/repository/npm-proxy/1gallery/-/1gallery-0.0.8.tgz
npm ERR! 403 In most cases, you or one of your dependencies are requesting
npm ERR! 403 a package version that is forbidden by your security policy. See https://npmjs.org/cli/audit for more details.
npm ERR! A complete log of this run can be found in:
npm ERR! /Users/nnandivelugu/.npm/_logs/2022-02-18T22-02-00.123Z-npm-install-1gallery-0.0.8.log
nnandivelugu@Navyasanthis-MacBook-Pro ~ %
```



Quarantine Report

2021-August-10 10:20 PM

Overview

The purpose of this report is to alert you of a component that has been quarantined due to a policy violation. No actions can be taken directly from this report, though you can remediate the component using the following information.

org.apache.logging.log4j:log4j-core:2.0.0

Status	Quarantine Reason	Repository
Quarantined	4 policy violations	Repository Name

First Quarantined	Catalogued Date	Other Versions in the Repository
1 month ago	4 years ago	4

Risk Remediation

Version Explorer

Popularity: Older, This Version, Newer

Breaking Changes: [Red bars]

Policy Threat Details: Security, License, Quality, Other

8.0.11

Compare Versions

CONDITION
Found security vulnerability CVE-2016-1000031 with severity >=9 (severity = 9.9)
Found security vulnerability CVE-2016-1000032 with severity >=7 (severity = 7.7)
Found security vulnerability CVE-2016-1003033 with severity >=4 (severity = 4.4)

Other Versions

COMPONENT

Org.apache.logging.log4j:log4j-core:2.11.5

개발자 Self Remediation

- 어떤 컴포넌트가 차단되었는지?
- 왜 차단되었는지?
- 어떻게 하면 차단되지 않는 컴포넌트를 선택할 수 있는지?

오픈소스 유입경로 및 점검

개발용 바이너리 오픈소스 패키지

Public Repos

Maven

npm

PyPI

nuget

RubyGems

설치형 오픈소스 패키지

Public Repos

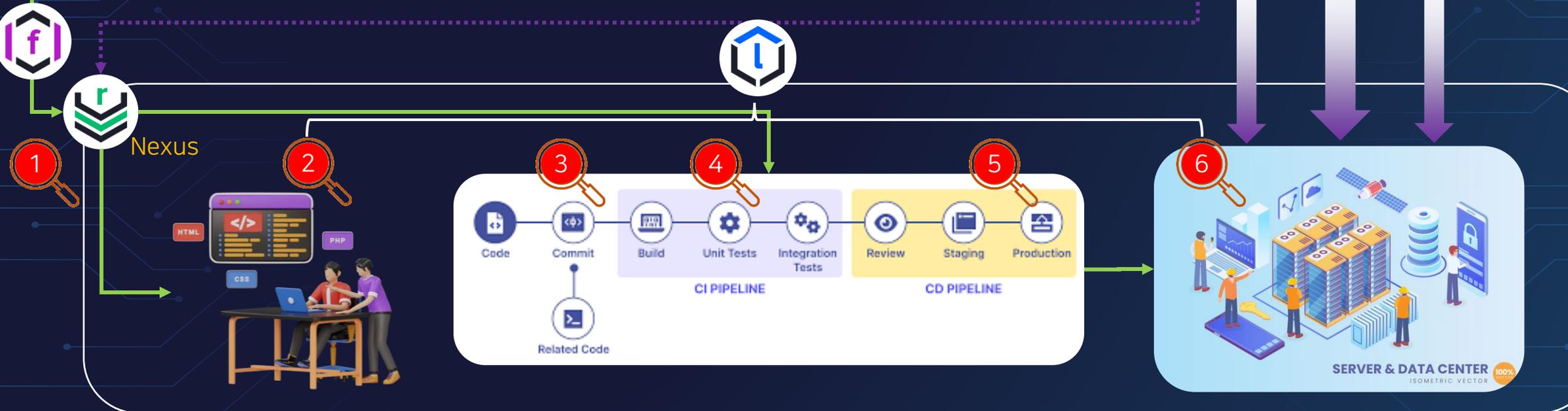
yum

apt-get

Docker

EPEL

Independent Repos



SCA (Software Composition Analysis)

(Sonatype Lifecycle, Blackduck, Mend, Labrado, Sparrow SCA)

Vulnerability Risk Management

(Nessus/Tenable, Rapid7, Qualys)

단계별 거버넌스 정책 적용

	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE
No Action	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Warn	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fail	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>



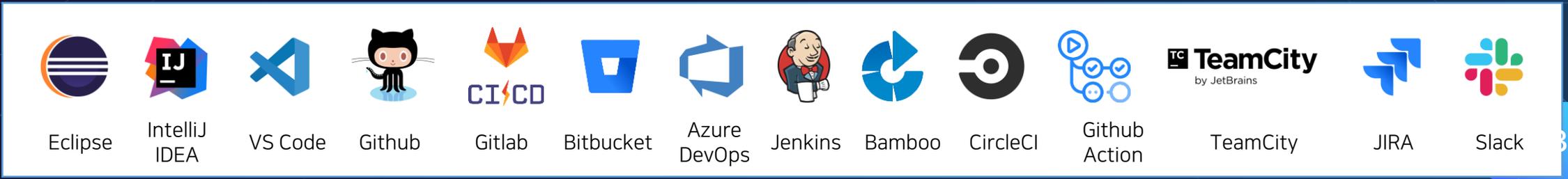
Actions

	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE
No Action	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Warn	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fail	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>				

Notifications

	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE	CONTINUOUS MONITORING
jaykim@osckore...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Recipient Type * Email *
 Email [v] thomas@osckorea.com [v] + Add



개발자 IDE 환경 지원



Eclipse



IntelliJ IDEA



VS Code



Visual Studio

The screenshot displays the IntelliJ IDEA interface with several panels. The 'Policy Violations' panel shows a table with columns 'Policy', 'Constraint', and 'Summary'. The 'License Analysis' panel shows a table with columns 'Threat Level', 'Declared License(s)', and 'Observed License(s)'. The 'Security Issues' panel shows a table with columns 'Threat Level', 'Problem Code', 'Status', and 'Summary'. The 'Component Info' panel shows details for 'commons-collections-3.2.1', including 'Declared License: Apache-2.0', 'Observed License: Apache-2.0', 'Effective License: Apache-2.0', 'Highest Policy Threat: 9 within 2 policies', 'Highest CVSS Score: 9', 'Cataloged: 10 years ago', 'Match State: exact', 'Identification Source: Sonatype', and 'Category: Programming Language Utilites'. A 'Popularity' chart and a 'Policy Threat' chart are also visible.

1 IDE 환경에서 Policy Violation을 유발하는 컴포넌트 확인

2 Breaking Changes : 업데이트에 코드변경이 필요한지 여부 확인

3 Version Explorer를 통해 최적의 컴포넌트 버전 선택

4 One-Click으로 보안 취약점 해소를 위한 마이그레이션

Source Control (형상관리시스템) 지원

- Commit에 대한 자동 피드백, Merge Blocking, 자동 Pull Request
- Breaking Changes 및 Transitive Dependency에 대해 포괄적인 수정 권고안



Azure DevOps



Bitbucket



GitHub



GitLab

Bump jackson-databind to 2.10.0 #4

collinpeters wants to merge 1 commit into master from b72286/com.fasterxml.jackson.core/jackson-databind/2.9.9.3-to-2.10.0

Conversation 0 Commits 1 Checks 0 Files changed 1

collinpeters commented 2 hours ago · edited · +@ · ...

Automated pull request to fix 1 Nexus IQ Policy Violation

Description

- Component: `com.fasterxml.jackson.core : jackson-databind`
- Current version (with violations): `2.9.9.3`
- New version (for remediation): `2.10.0`

Policy

Threat (of 10)	Policy	Constraint	Violation Details
10	Security-Critical	Critical risk CVSS score	Found security vulnerability <code>CVE-2019-17267</code> with severity <code>>= 9</code> (severity = 9.8).

Nexus IQ Scan Detail

Application: My App
Organization: My Organization
Date: 2019-11-27 13:58:11 GMT-8
Stage: build

Review full report

This PR was automatically created by your friendly neighbourhood IQ Server

Automated pull request: Nexus IQ found 3 Policy Violations

Description

- Component: `org.apache.logging.log4j : log4j-core`
- Current version (with violations): `2.4`
- New version (for remediation): `2.13.3`
- **Multiple breaking changes** - This version upgrade may require significant effort.

All checks have failed 1 failing check [Hide all checks](#)

IQ Policy Evaluation — Components: Critical: 14, Severe: 8, Moderate: 2 **Required** [Details](#)

Required statuses must pass before merging
All required [statuses](#) and check runs on this pull request must run successfully to enable automatic merging.

As an administrator, you may still merge this pull request.

Merge pull request You can also [open this in GitHub Desktop](#) or view [command line instructions](#).

parent 085beb18 master

Pipeline #75179799 failed with stage **IQ Policy Evaluation - Components: Critical: 14, Severe: 8, Moderate: 2**

IQ Policy Evaluation

Changes 1 **Pipelines 1**

CI Integration (e.g. Jenkins)

Jenkins Script (설정)

```
nexusPolicyEvaluation(  
    iqApplication: 'SampApp',  
    iqInstanceId: 'MyNexusIQServer1',  
    iqScanPatterns: [[scanPattern: '**/*.js'], [scanPattern: '**/*.zip']],  
    iqStage: 'build',  
    iqOrganization: '55040769ec08424e84049356a3362d07'  
)
```

ACTIONS							
ACTION	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE
No Action	<input checked="" type="radio"/>						
Warn	<input type="radio"/>						
Fail	<input type="radio"/>						

NOTIFICATIONS								
RECIPIENT	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE	CONTINUO... MONITORING
No notifications configured								

Jenkins Build 리포트

Nexus IQ Build Report
This report lists IQ policy violations which are configured to 'warn' or 'fail'. [See full report in IQ Server](#)

Application: test123
Stage: build

7 Build Failures caused by 2 components
55 Warnings caused by 41 components

[See Policy Violations directly in your IDE](#)
[IDEA](#) [Visual Studio](#) [Eclipse](#)

THREAT / POLICY NAME	ACTION	CONSTRAINT	CONDITION
10 Security-Critical	Fail	Critical risk CVSS score	Found security vulnerability CVE-2019-17267 with severity 9.8.
9 Security-High	Fail	High risk CVSS score	Found security vulnerability CVE-2019-14540 with severity 7.5. Found security vulnerability CVE-2019-14540 with severity 7.5.
9 Security-High	Fail	High risk CVSS score	Found security vulnerability CVE-2019-14892 with severity 8.5. Found security vulnerability CVE-2019-14892 with severity 8.5.
9 Security-High	Fail	High risk CVSS score	Found security vulnerability CVE-2019-14893 with severity 8.5. Found security vulnerability CVE-2019-14893 with severity 8.5.
9 Security-High	Fail	High risk CVSS score	Found security vulnerability CVE-2019-16335 with severity 7.5. Found security vulnerability CVE-2019-16335 with severity 7.5.
9 Security-High	Fail	High risk CVSS score	Found security vulnerability sonatype-2019-0371 with severity 8.5. Found security vulnerability sonatype-2019-0371 with severity 8.5.

THREAT / POLICY NAME	ACTION	CONSTRAINT	CONDITION
10 Security-Critical	Fail	Critical risk CVSS score	Found security vulnerability sonatype-2019-0115 with severity 9.8.
7 Security-Medium	Warn	Medium risk CVSS score	Found security vulnerability CVE-2018-14042 with severity 6.1. Found security vulnerability CVE-2018-14042 with severity 6.1.

IQ Server를 통한 Full Report 확인

IDE를 통한 Policy Violation 확인

자동화된 오픈소스 관리체계를 위한 세부요건



Shift Left (시프트 레프트)

오픈소스 유입 관문부터 실시간 통제



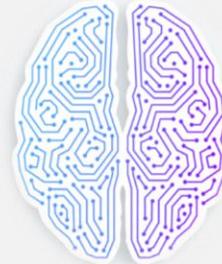
개발자 스스로 최적의 컴포넌트 선택



Accuracy (정확성)

글로벌 최대 데이터베이스 운영

- Maven 운영관리 주체
- NPM/PYPI AI/ML 모니터링
- +65명의 전문 보안연구원
- 전세계 최대 Repo 공급사



Advanced Binary Fingerprint 식별 기술



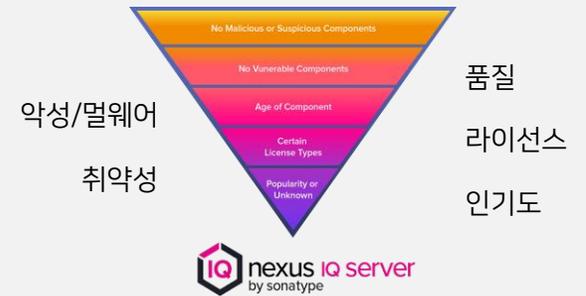
```
<item key="013b4d333e95f3a5ac765fc2a3ab05e9f29d7952"
path="ch/qos/logback/core/util/Loader.class"
sha1="6cdbcfa9150af71c7b6b3adfbbce1e940f9413e"
sha1JA001="2f9768f33c106400ae23863165643d167a25e8ba"
sha1JB001="878d54d1c132ddee47ec7ebd9cefbdb31cb5ac"
sha1JC001="f65040a6798ab66c56ce0ef163195454a68c5921"
sha1JD001="4f093c9bd65a0e6d233171b3362109ab5b372235"/>
```

자동화 필수요건



Flexible Policy (유연한 정책)

다양한 속성을 통한 정책 정의



단계별 차등화 된 정책 적용

ACTIONS	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE
No Action	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Warn	<input type="radio"/>						
Fail	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Beyond SDLC SBOM Manager

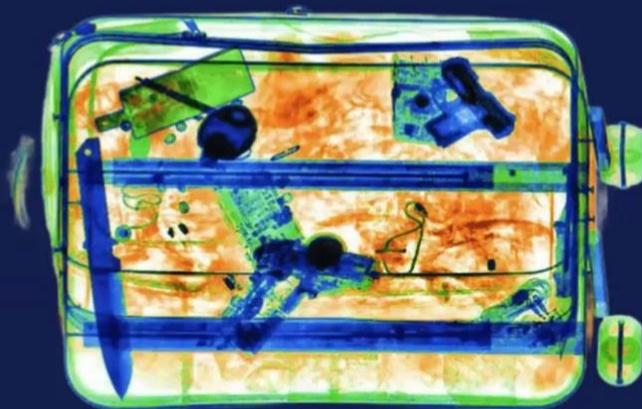
- ✔ 소프트웨어 공급망 관리의 도전과제 및 공격 기법
- ✔ 오픈소스 거버넌스 자동화 고려사항
- ✔ 오픈소스 거버넌스 자동화 구현 방안
- ✔ SBOM 통합관리를 위한 SBOM Manager



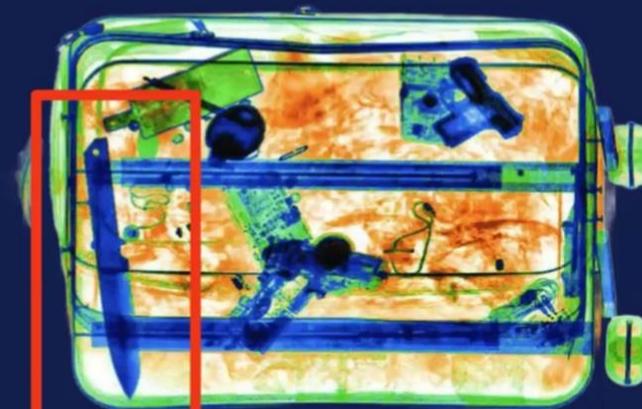
Software Composition Analysis



Identify
Contents



Identify
Threats

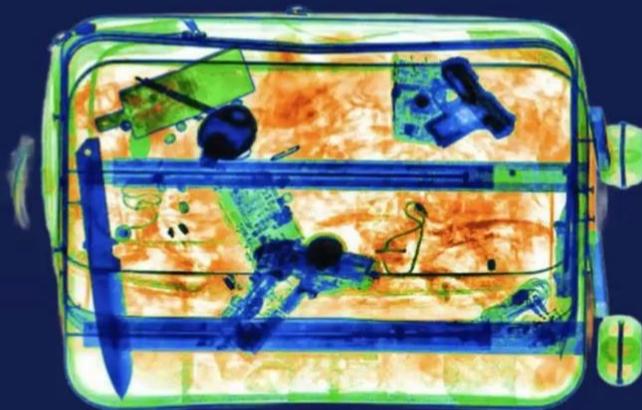


Vulnerable
Log4j

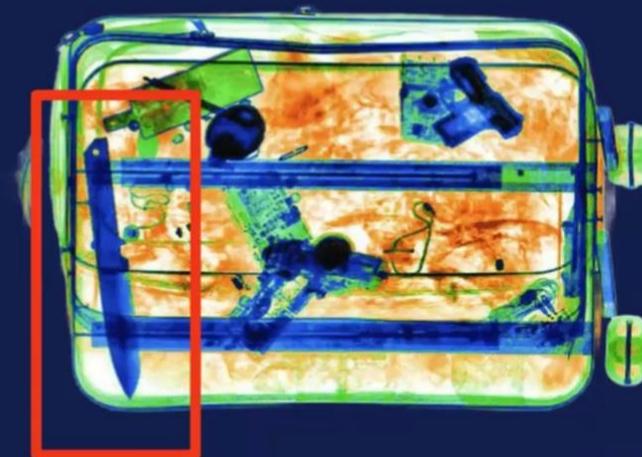
Software Composition Analysis



Identify
Contents

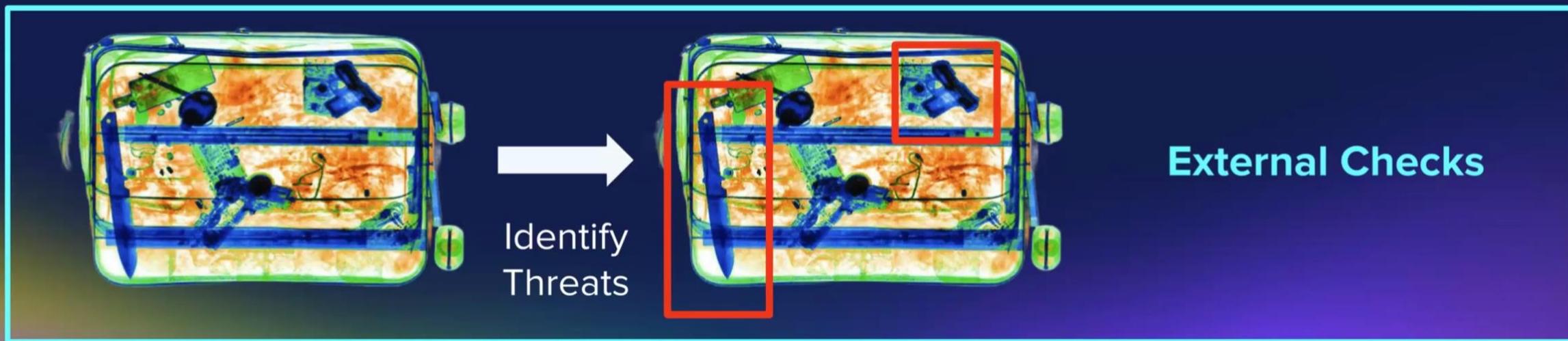
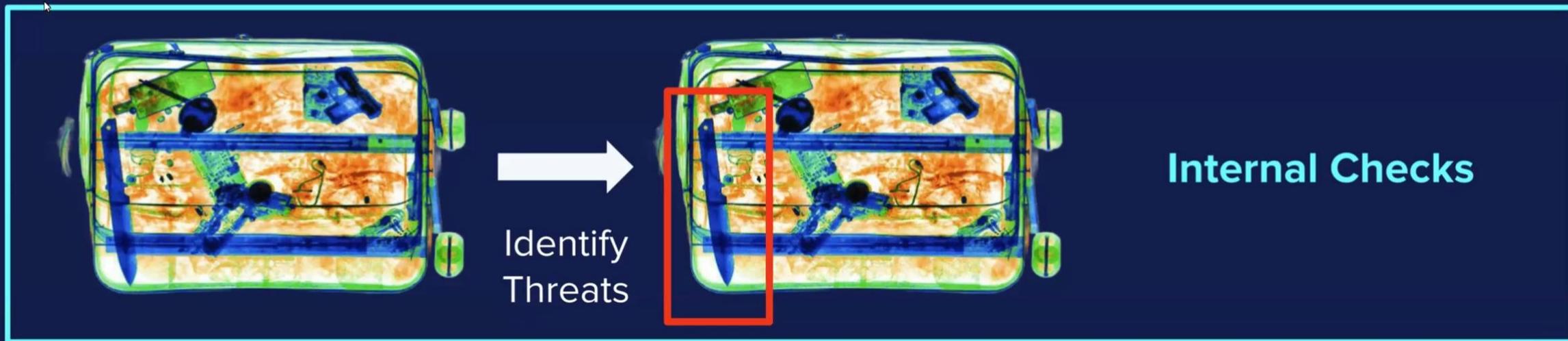


Identify
Threats



**Software Bill of
Materials (SBOM)**
makes this shareable

Checking Your Work



Regulations: You Need SBOM Manager If...



신용카드 사용자 데이터를 저장,처리 및 전송하는 경우
(PCI 4.0)



EU에 소프트웨어가 포함된 유형의 제품을 판매하는 경우
(CRA)



EU에서 디지털서비스를 운영하거나 중요한 산업을 지원하는 경우
(NIS2)



금융기관이거나 금융조직을 지원하는 경우
(DORA)



의료장치를 판매하는 경우
(FD&C Act / FDA)



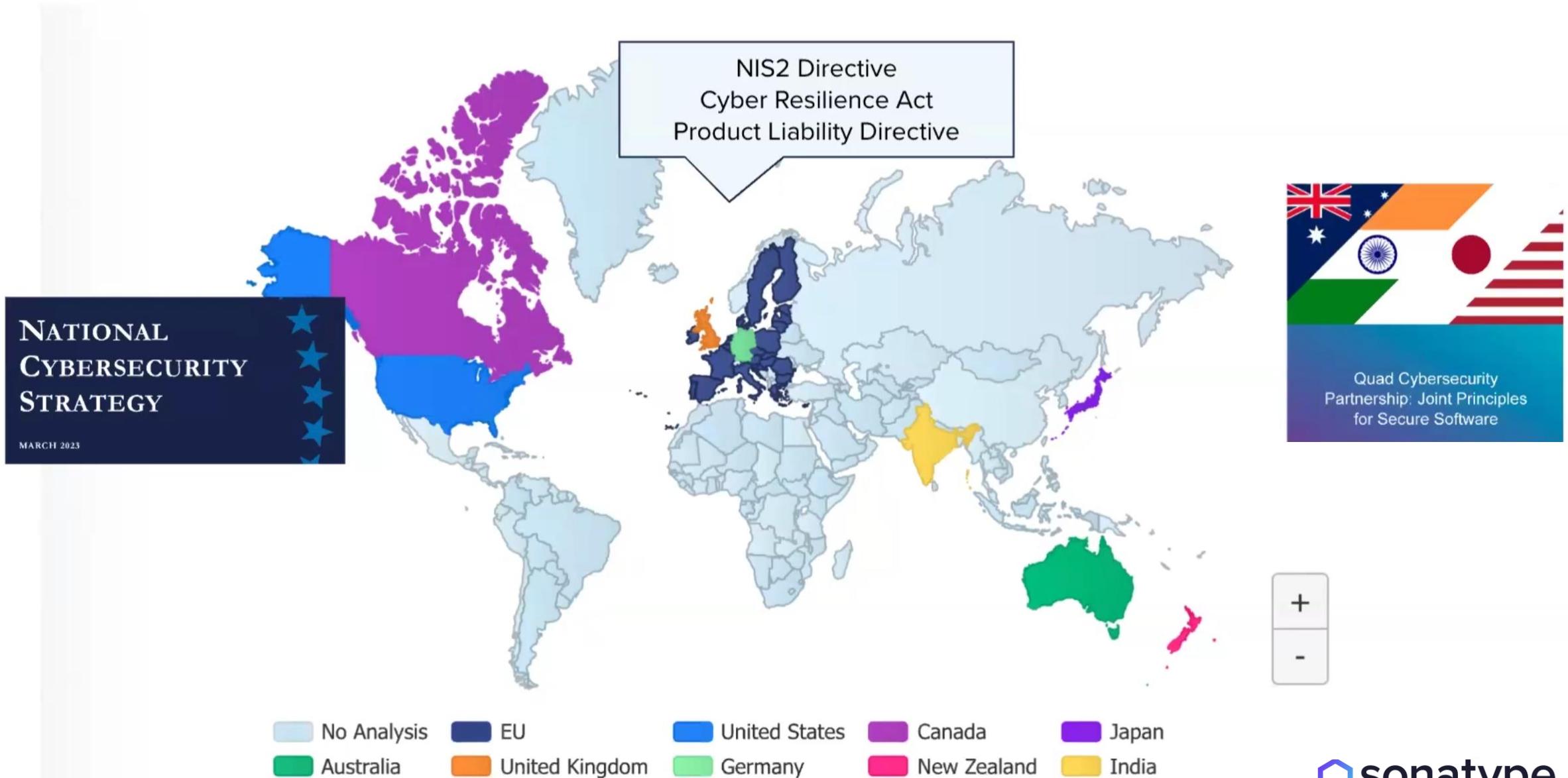
미국 연방정부에 소프트웨어를 판매하는 경우
(CISA Attestation Form)



미국 연방정부를 위한 계약 건으로 소프트웨어를 개발하는 경우
(FAR)



Regulations Are Coming Here



표준 SBOM

Application 분석 Report는 CycloneDX 또는 SPDX 포맷의 SBOM 형태로 생성할 수 있습니다.

Options

- Export PDF
- Export CycloneDx
- Export SPDX
- [View raw data](#)
- [View vulnerabilities](#)
- [View legacy report](#)

```
C:\Users> jayki > Downloads > | webgoat-build-97c3cf64728d41eb8d78881d453caa07\spdx (1).json > ...
1
2 "SPDXID": "SPDXRef-DOCUMENT",
3 "spdxVersion": "SPDX-2.3",
4 "creationInfo": {
5   "created": "2024-01-24T06:10:03Z",
6   "creators": [ "Tool: Sonatype IQ Server - 1.165.0-01" ]
7 },
8 "documentNamespace": "http://192.168.41.50:8070/ui/links/application/webgoat/report/97c3cf64728d41eb8d78881d453caa07",
9 "packages": [ {
10   "SPDXID": "SPDXRef-maven-org.webjars.jquery.3.5.1",
11   "externalRefs": [ {
12     "referenceCategory": "PACKAGE-MANAGER",
13     "referenceLocator": "pkg:maven/org.webjars/jquery@3.5.1?type-jar",
14     "referenceType": "purl"
15   } ],
16   "filesAnalyzed": false,
17   "licenseConcluded": "(MIT AND UNKNOWN)",
18   "licenseDeclared": "(MIT AND UNKNOWN AND No-Source-License)",
19   "name": "org.webjars.jquery",
20   "versionInfo": "3.5.1"
21 }, {
22   "SPDXID": "SPDXRef-maven-com.fasterxml.jackson.core.jackson-annotations-2.13.3",
23   "externalRefs": [ {
24     "referenceCategory": "PACKAGE-MANAGER",
25     "referenceLocator": "pkg:maven/com.fasterxml.jackson.core/jackson-annotations@2.13.3?type-jar",
26     "referenceType": "purl"
27   } ],
28   "filesAnalyzed": false,
29   "licenseConcluded": "Apache-2.0",
30   "licenseDeclared": "Apache-2.0",
31   "name": "com.fasterxml.jackson.core:jackson-annotations",
32   "versionInfo": "2.13.3"
33 }, {
34   "SPDXID": "SPDXRef-maven-org.bouncycastle.bctls-jdk15on-1.68",
```

CycloneDX (bom.xml)

```
C:\Users> jayki > Downloads > | webgoat-bom (1).xml
1 <?xml version="1.0" encoding="UTF-8"?>
2 <bom serialNumber="urn:uuid:97c3cf64-728d-41eb-8d78-881d453caa07" version="1" xmlns="http://cyclonedx.org/schema/bom/1.4">
3   <metadata>
4     <timestamp>2023-11-06T08:34:35Z</timestamp>
5     <tools>
6       <tool>
7         <vendor>Sonatype Inc.</vendor>
8         <name>Nexus IQ Servers</name>
9         <version>1.165.0-01</version>
10      </tool>
11    </tools>
12    <component type="application" bom-ref="79d938b8-84f2-4f3e-be0a-8528e9fce4cf">
13      <group>sonatype</group>
14      <name>iq_application_webgoat</name>
15      <version>97c3cf64728d41eb8d78881d453caa07</version>
16      <purl pkg:generic/sonatype/iq_application_webgoat@97c3cf64728d41eb8d78881d453caa07/>
17    </component>
18    <properties>
19      <property name="Scan ID">97c3cf64728d41eb8d78881d453caa07</property>
20    </properties>
21  </metadata>
22  <components>
23    <component type="library" bom-ref="e66f17c-def3-48bb-8f85-5eacc391c192">
24      <group>com.github.jnr</group>
25      <name>jnr-x86asm</name>
26      <version>1.0.2</version>
27      <licenses>
28        <license>
29          <id>MIT</id>
30        </license>
31      </licenses>
32      <purl pkg:maven/com.github.jnr/jnr-x86asm@1.0.2?type-jar/>
33      <modified>false</modified>
34    </component>
35    <property name="Sonatype truncated SHA1">006936bbd6c5b235665d</property>
36    <property name="Match State">exact</property>
37    <property name="Identification Source">Sonatype</property>
38  </components>
39 </bom>
```

SPDX (bom.json)

test2app Build Report

Triggered by Continuous Integration on 2023-06-08 16:56:48 UTC-0500 - Commit: fc161791bcbaf170d6ce03b6d91a47b45a9613e4

357 663 1020 VIOLATIONS Affecting 831 components 1278 COMPONENTS 83% of all components identified 1526 LEGACY VIOLATIONS

Aggregate by component View Dependency Tree Filter

THREAT	POLICY	COMPONENT
10	Security-Critical	c3p0 : c3p0 : 0.9.1.1
10	Security-Critical	com.fasterxml.jackson.core : jackson-databind : 2.2.2
10	Security-Critical	com.h2database : h2 : 1.3.176
10	Security-Critical	commons-collections : commons-collections : 3.2.1
10	Security-Critical	commons-fileupload : commons-fileupload : 1.3.1
10	Security-Critical	dom4j : dom4j : 1.6.1
10	Security-Critical	handlebars : 1.0.12
10	Security-Critical	log4j : log4j : 1.2.16



sonatype lifecycle



WHERE COMPONENTS COME FROM



CI/CD INTEGRATION



IDE INTEGRATION



SCM INTEGRATION

WHAT RISKS ARE ENTERING MY PIPELINE?
WHERE WILL I BE BLOCKED IN THE SDLC?



정책준수 평가

수정방안에 대한 가이드

배포정책 준수여부 확인

배포 버전의 지속적인
컴플라이언스 준수 여부 확인



수정/치유



정책 적용
- Legal
- Security
- Quality



지속적인 모니터링

Dev

Build

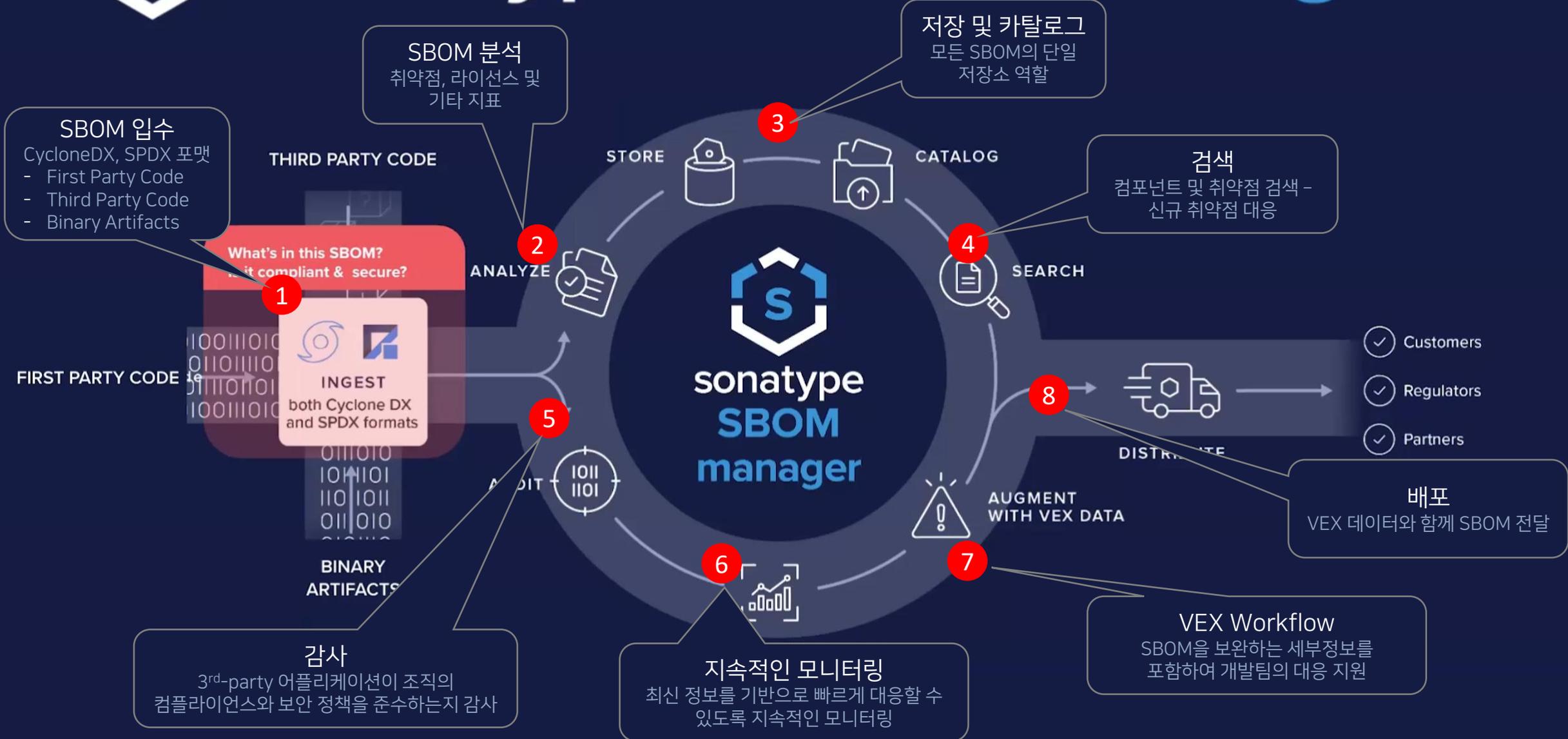
Test

Release

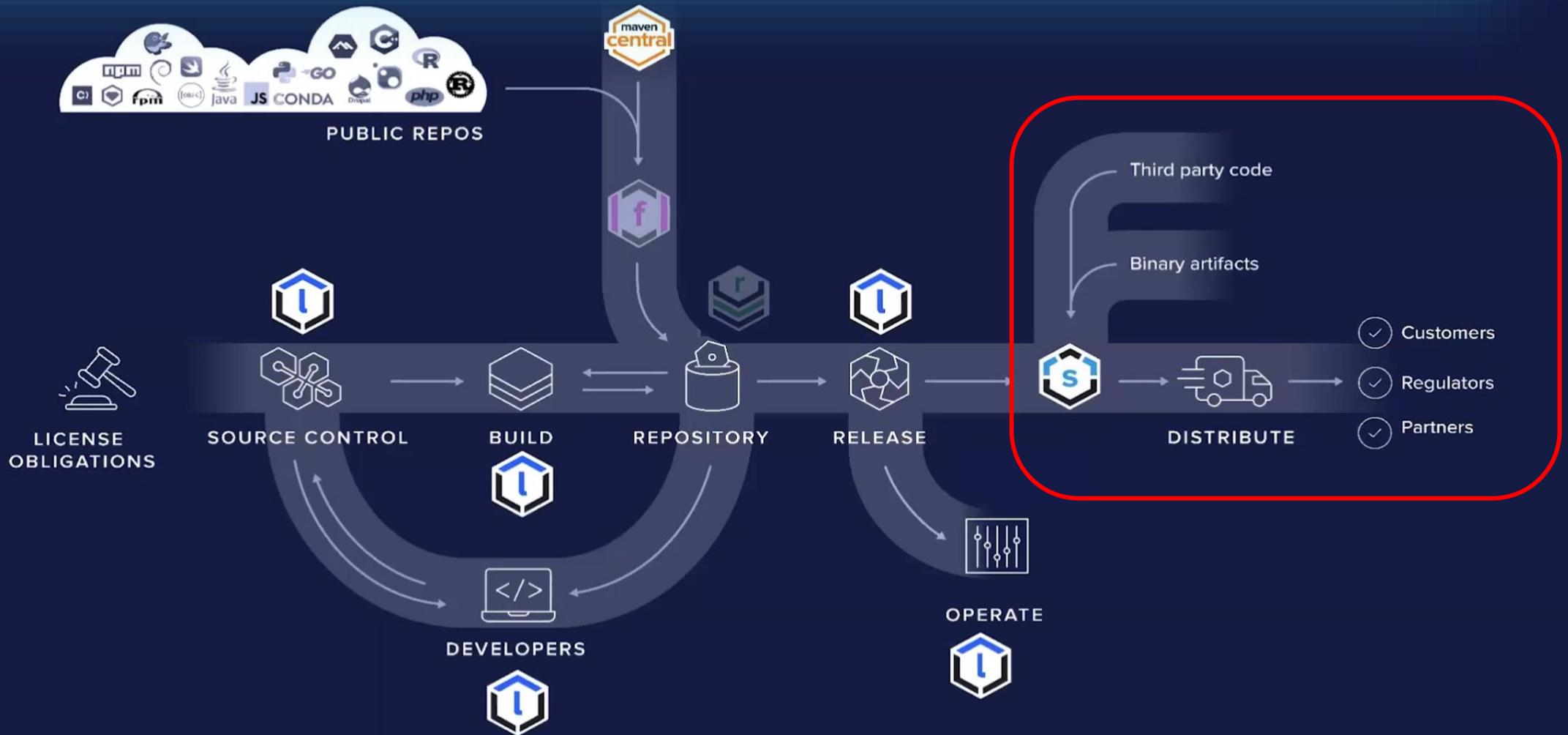
Operate



sonatype SBOM manager



The essential duo of SCA and SBOM management



DEVSECOPS PIPELINE

SBOM COMPLIANCE

VEX Annotations

SELECT

In triage

Exploitable

False positive

Annotate CVE-2021-42392

pkg:maven/com.h2database/h2@1.4.196?type=jar

CVSS Score 9.8 Verification Status Sonatype Verified

Description

The org.h2.util.Util.getConnexion method of the H2

SELECT

Disclosed Vulnerabilities

Existing vulnerabilities disclosed by the originator of this SBOM.

CVSS SCORE	ISSUE	VERIFIED STATUS	ANALYSIS STATUS	JUSTIFICATION	ACTION
9.8	CVE-2021-42392	Sonatype Verified	In Triage	Requires configuration	Edit
9.8	CVE-2022-23221	Sonatype Verified	Unannotated		Add
9.8	sonatype-2018-0859	Sonatype Verified	Unannotated		Add
6	sonatype-2018-0863	Sonatype Verified	Unannotated		Add

rollback

workaround_available

Save

Sonatype SBOM Manager vs. SCA

Software Composition Analysis

Part of the SDLC

개발 파이프라인에서 Legal, security, Quality 리스크가 없는 최적의 컴포넌트를 선택하기 위해 활용

최종 버전 관리

Development (SDLC) 중심

Remediation 중심

주사용자 : 개발팀, 보안팀, DevOps팀

SBOM Management

Beyond the SDLC

배포된 소프트웨어를 관리하고, 필요시 패치를 반영하거나 요청할 수 있도록 소프트웨어 개발 생명주기 이후 버전별로 관리

배포된 모든 버전에 대한 관리

Release / Deployment 중심

Compliance 중심

주사용자 : 컴플라이언스, 구매팀, 및 보안팀

감사합니다

OSC Korea